МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря Сікорського»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ЛАБОРАТОРНА РОБОТА №2

з дисципліни «Криптографія»

Варіант 3

Виконали:

Студенти групи ФБ-92

Шевченко Семен та

Щур Павло

Київ 2021

Завдання

Мета роботи:

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера

Постановка задачі:

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

Для виконання першого та другого пункту завдання був використаний текст Януша Пшемановського «Четыре танкиста и собака», який був попередньо оброблений з метою виключення всіх символів, що не входять в початковий алфавіт. В другому пункті завдання було проведено обрахунки індексу відповідності для текстів зашифрованих ключами різної довжини . Наведені нижче графіки зображують залежність індексу відповідності від довжини ключа.

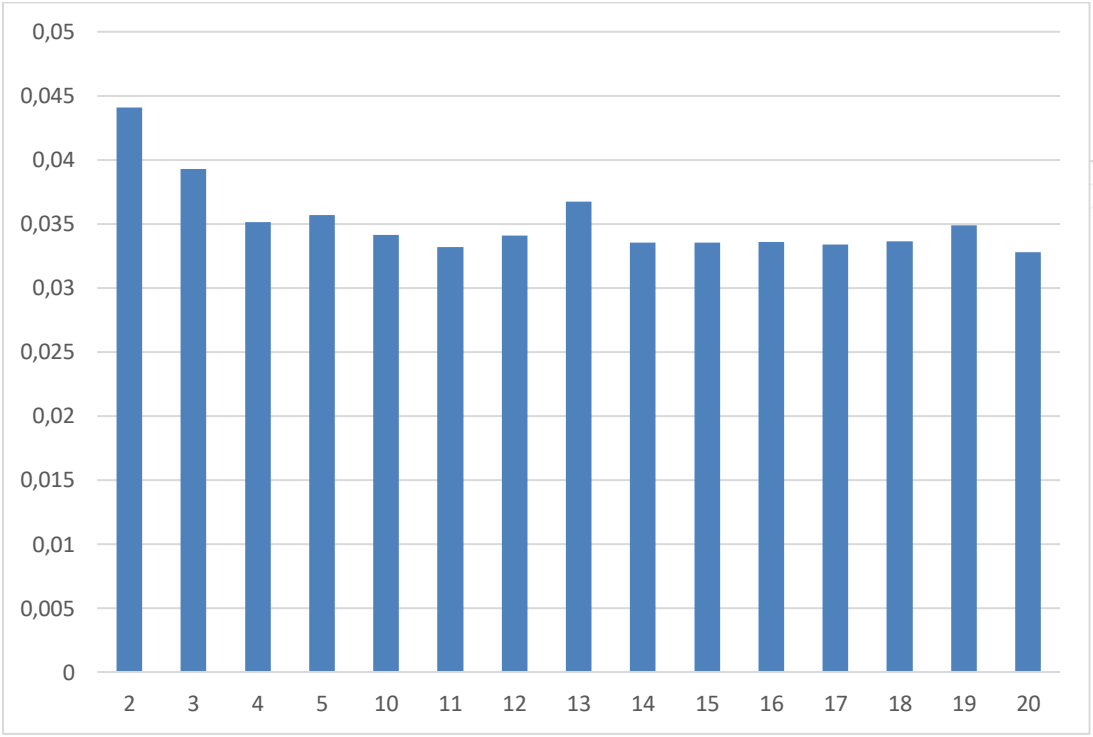
1
Частина

Довжна ключа	Ключ	Зашифрований текст
2	да	Гнчшушммднтвхкмймзжехтсынптласоинвтесняйуихацепьмжчрсапихтдвцофмсозищртм…
3	нет	Мтеефкхстъуфюпъцнщпкгятнцфашбгчныпучътнцфъюедтрохлеэттшнгяефяувщтарнзэу…
4	шкаф	Ччумзвиашчоцйфиэасвщйьнпбщояфыкьбмощечыэзтсфкплрарудекльйьацкшраешгьнъ…
5	повар	Оыхшязцоаээрукшшцйвхаапыщюьньбщцлвюфыпыщюцуавфщюицвюпаычяфатбьтмээс…
10	специалист	Рьшочшуфсяясцарйупучвбтсспщунгычошцешхмыачццъецдщшдятцуиьъсфгэхвхооржвяыегцвъ…
11	абрикосовый	Яогащжщъвичвтъруцшрзмыньщчшщнямгтвпххчйъэкмйтжыдтфдюпыфитвимаяюоичгйе…
12	квалификация	Йпугчмрцагцбымифрыкпсихъусоцдеттйшцдчпыфчьщктыуытиуыхфутсиибьррчхвлтхжцлкпончвк…
13	авианавигация	Япышьшкфгндкрккксифвзщхнссоондсчилксегхъйсрснтзуяиьыпнвуиютвкхожфмоерхэооирош…
14	автоматический	Япежышъфчтямщуилъхоегъдаъщцфьуьцхвандтмучссвдучьъокхюкуссфтрюовфдуфтэщ…
15	агроконференция	Яргжщжхаеэупзтзйлчрпяябащфыбдрклщршуъбащфхзисеомцрбэбеынюиибтсаъчьрьъаущ…
16	безответственный	Атъжбънюсярзючгтймйугфтнъбррйюескзхуяпаыаъуеятжейлъюявръвдвзяылхоукцзтуюся…
17	автопроизводитель	Япежюицфзпьжщьнфдздчябэйсцрщащьнфюозяыкщэршвайуонспрптщчбаийфьффяуодхт…
18	агропромышленность	Яргжюицшыещзючцъъгвибаьлчыйгзцчхчуабнрлчюшямнэцбхуббяьллбаптаълдшурхгба…
19	антропоцентричность	Яъеиэзцвеъатщбхчщщюеюдэйшэдрйгърапьцяйыцбшяпаырйъцызъоьънтнфвьяъгуръеше…
20	воздухонепроницаемый	Быъьвнцщеьюрютюйнуэоуафяьдьшбаъццкдетщцтсцшдеъщйнхгюъибицюылфьчрагсхъяю…

Частина 2

Індекс відповідності відкритого тексту: 0.054

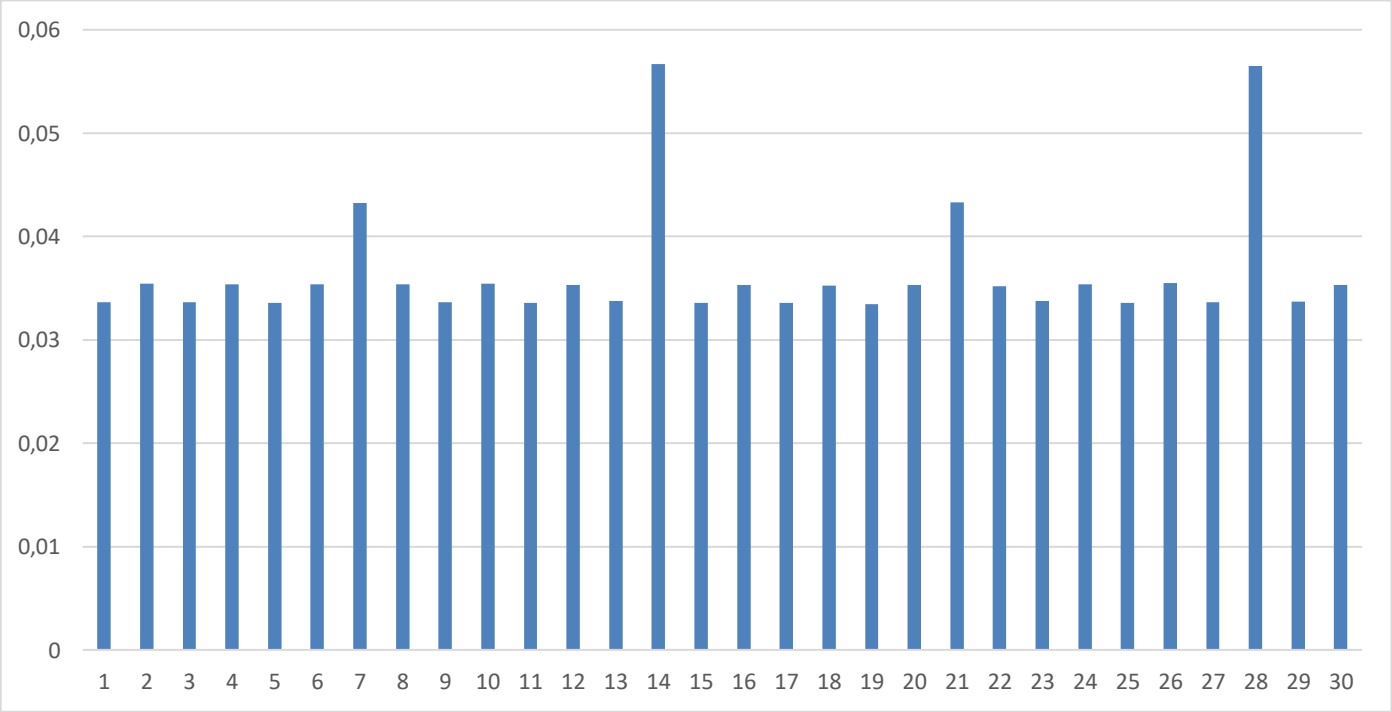
Довжина	Ключ	Індекс відповідості
2	да	0.044073252490553806
3	нет	0.03928207645233862
4	шкаф	0.03512091548424572
5	повар	0.03570521906817672
10	специалист	0.0341543009568549
11	абрикосовый	0.03316977366178033
12	квалификация	0.03410488961560226
13	авианавигация	0.03675708840951929
14	автоматический	0.033547913081509007
15	агроконференция	0.03354667116208517
16	безответственный	0.033561626996990536
17	автопроизводитель	0.033395531154932004
18	агропромышленность	0.03362750927653418
19	антропоцентричность	0.03489952113920576
20	воздухонепроницаемый	0.03279385563273878



Частина 3

Для виконання третього завдання текст було розбито на 30 блоків. Програмно було знайдено блок, відповідність якого найближча до теоретичного значення індексу відповідності (0.054) звідси отримуємо довжину ключа 28. Надалі за методичними вказівками шукаємо сам ключ. Отримано ключ «эбомацтникфуьоэйомдятниофубо», можна зробити висновок що ключ є подвійним , використаймо ключ “эбомацтникфуьо”, За допомогою умови змістовності було визначено ключ: “экомаятникфуко”

Довжина ключа	Індекс відповідості	Довжина ключа	Індекс відповідості
1	0.03365878060005469	16	0.03532923505501202
2	0.03540318621049883	17	0.033553157074346744
3	0.033657628252257855	18	0.035250813284029715
4	0.03537512674612907	19	0.03342913541516716
5	0.03360074463931021	20	0.035329220456214554
6	0.035353382712172456	21	0.043282276072429494
7	0.04321232340902984	22	0.035165903720665165
8	0.035366115767448164	23	0.03377602673928392
9	0.03361816528900438	24	0.03536201414470406
10	0.035441203962855314	25	0.03359764522859079
11	0.03357008893142104	26	0.03550495354771452
12	0.03527913582243025	27	0.033646448144021054
13	0.033742872053219006	28	0.05646761560900226
14	0.05667060702875398	29	0.0336932257727597
15	0.03355059522920367	30	0.03529422809190424



В результаті розшифрування було отримано уривок з твору Умберто Еко “Маятник Фуко“. Отриманий відкритий текст:

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличииописывалколеб
аниязналноивсякийощутилбыподчарамимернойпульсациичтопериодколебанийопределенотношениемквад
ратногокорнядлинынитикчислуркотороеиррациональноедляподлунныхумовпредлицомбожественнойрацио
неукоснительносопрягаетокружностисдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшар
аотодногополюсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеевневременных
мерединственноститочкикрепленияздвойственностиабстрактногоизмерениятроичностичислапискрытойчетв
еричностиквадратногокорнясовершенствакругаещеязналчтонаконцеотвеснойлинииивосстановленнойотточк
икреплениянаходящийсяподмаятникоммагнитныйстабилизаторвоссылаеткомандыжелезномусердцушараио
беспечиваетвечностьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивлениематериинокоторая
непротиворечитзаконуфуконапротивпомогаетемупроявитьсяпотомучтопомещенныйвпустотулюбойточечн
ыйвеспринженныйкконцунерастяжимойиневесомойнитиневстречающийнисопротивлениявоздуханитрени
явточкекрепленияйдействительнобудетсовершатьрегулярныеигармоничныеколебаниявечномедныйшарпоиг
рывалбледнымипереливчатымиотблескамиподпоследнимилучамишедшимиизвитражаеслибыкаккогдатоонк
асалсяслоямокрогопесканаплитахполаприкаждомизегокасанийпрочерчивалсябыштрихиэтиштрихинеулови
моизменяякаждыйразнаправлениерасходилисьбыоткрываяразломытраншеирвыиугадываласьбырадиальная
симметричностькостякмандалыневидимаясхемапентакулазвездымистическойрозынетнетэтобылабынерозаэ
тобылбырассказзаписанныйнаполотнахпустыниследаминесосчитанныхкаравановповестьотысячелетнихски
танияхнаверноеэтойдорогойшлиатлантыконтинентамувугрюмойупорнойрешительностиизтасманиивгренла
ндиюоттропикакозерогактропикуракасостроваприцаэдуарданашпицбергенкасаниямишараутрамбовывалос
ьминутныйрассказвсечтоонитворилвпромежуткахотодноголедовогопериодадодругогоискореевсеготворя
твнашевремясделавшисьрабамиверховниковвероятноперелетаяотсамоаноновуюземлюэтотшарнацеливается
вапогеепараболынаагартуцентрмираячувствовалкактаинственнымобщимпланомобъединяетсяавалонгиперб
ореевсполуденнойпустынейоберегающейзагадкуайерсроквданныймигвчетыречасаднядвадцатьтретьегоиюн
ямаятникутрачивалскоростьукраяколебательнойплоскостибезвольноотшатывалсяснованачиналускоряться як
центруинаразгонепосерединерассекалссабельнымсвистомтайныйчетвероугольниксилопределявшихегосудь
буеслибыяпробылтамдолгонеуязвимыйдлявременинаблюдаякакэтаптичьяголоваэтоткопейныйнаконечникэ
тотопрокинутыйгребеньшлемавычерчиваетвпустотесвоидиагоналиотраядокраяастигматическойзамкнутой
линиияпревратилсябывжертвуобольщениячувствимаятникубедилбыменячтоколебательнаяплоскостьсовер
шилаполныйоборотивозвратилаьвпервоначальноеположениеописавзатридцатьдвачасасплюснутыйэллипсэ
ллипсобращающийсявокругсобственногоцентраспостояннойугловойскоростьюпропорциональнойсинусуге
ографическойширотыкаквращалсябытотжеэллипсбудьнитьмаятникаприкрепленаквенцухрамасоломонаверо
ятнорыцариииспробовалииэтоможетбытьихрасчеттоестьконечныйрезультатрасчетанеизменялсяможетбытьс
обораббатствасенмартендешанэтодействительноистинныйхрамвообщечистыйэкспериментвозможентолько
наполюсеэтоединственныйслучайкогдаточкаподвешиванянитирасположилаьбынапродолженииземнойос
иимаятникзаключилбысвойвидимыйциклровновдвадцатьчетыречасаоднакоэтоотступлениеотзаконактомуж
епредусмотренноесамимзакономэтапогрешностьпротивзолотойнормыневотнималачудесностиучудаязналчто
земляврашаетсяичтоявращаюсьвместеснеюисенмартендешанивесьпарижсомноюивсемывращалисьподмаят
никомкоторыйдействительнонисколькоиземенялориентациисвоегопланапотомучтонаверхугдеонкчемутоб
ылпривязаннадругомконцевоображаемогобесконечногопродолженияянитиввысотуивдальзапределамиотдале
нныхгалактикнаходилаьнедвижимаяинепреложнаявсвоейвековечностимертваяточказемлядвигаласьоднако
местоккоторомуприкреплялсяканатбылоединственнымнеподвижнымместомвселеннойпоэтомумойвзглядбы
лприкованнестолькокземлесколькокнебуосиянномутайнойабсолютнойнеподвижностимаятникговорилмнеч
тохотявращаетсявсеземнойшарсолнечнаясистематуманностичерныедырыилюбыепорожденияграндиознойк
осмическойэманацииотпервыхэоновдосамойлипучейматериисуществуеттолькооднаточкаосьнекийшампурз
анебесныйштырьпозволяющийостальномумируобращатьсяоколосебяитеперьяучаствовалвэтомверховномоп
ытеявращавшийсякаквсенасветесообщасовсемнасветеудостаивалсявидетьтонедвижноекрепостьопорусвето
носноеявлениекотороенетелесноинеимеетнигранцыниформынивесаниколичестваникачестваиононевидитн
еслышитнеподдаетсячувственностиинепребываетнивместенивовременинивпространствеиононедушанеразу

мневоображениенемнениенечислонепорядокнемеранесущностьневечностьононетьмаинесветононеложьине истинадоменядолетелпасмурныйобменрепликамимеждупарнемвочкахидевицейувыбезочковэтомаятникфук оговорилеемилыйпервыйопытпроводиливпогребевтысячавосемьсотпятьдесятпервомгодупотомвобсерватор иипотомподкуполомпантеонадлинаканаташестьдесятсемьметроввесгиридвадцатьвосемькилонаконецвтыся чавосемьсотпятьдесятпятомподвешентутвуменьшенномасштабеканатпротянутчерезнижнююючастьзамкасв одаазачемнадочтобыонболталсядоказываетсявращениеземлипосколькуточкакрепленияянеподвижнаапочему онанеподвижнапотомучтоточкасейчасятебеобъяснювцентральнойточкелюбойточкенаходящейсясредидруги хвидимыхточеквобщемэтоуженефизическаяточкаакакбыгеометрическаяитыеенеможешьвидетьпотомучтоу неенетплощадиатоучегонетплощадинеможетперекоситьсянивлевонивправоникверхуникнизупоэтомуонанев ращаетсясследишьеслиуточкинетплощадионанеможетповорачиватьсявокругсебяунеенетэтогосамогосебяноэ таточканаземлеаземлявертитсяземлявертитсяаточканевертитсяможешьневеритьеслиненравитсяясномнекак оеделонесчастнаяиметьнадголовойединственнуюстабильнуючастицумиратонисчемнесравнимоечтонеподве рженопроклятиюобщегобегаисчитатьчтоэтонееаегоделовследзаэтимчетапошлапрочьонобнимаясвойсправо чникотучившийегоудивлятьсяонаволочасвойорганизмглухойксердцебиениюбесконечностииобаникакнепыт аясьзакрепитьвпамятиопытэтойвстречиихпервойиихпоследнейсединымсэнсофсневысказуемымонинепалин аколенипередалтаремистиныягляделсвниманиемистрахомимнеповерилосьчтоякопобельбоправвсегдашниее годифирамбымаятникуяпривыксписыватьнабесплодноеэстетствозлокачественноекотороемедленноразъедал оегодушуибесформенноеперенималоформуеготеланезаметноперекодируяигрувреальностьжизниоднакоесли бельбобылправнасчетмаятникавероятноонбылправинасчетвсегопрочегоибылпланибылвсеобщийзаговориб ылоправильночтояоказалсяздесьсегоднянаканунелетнегопротивостоянияякопобельбонесумасшедшийемупр остопривелосьвовремяигрычерезигруоткрытьистинуделовтомчтосопричастностьбожескомуневожетпродол жатьсядолгонепотревоживрассудоктогдаяпостаралсяотвестивзглядпрослеживаядугукотораяоткапителейрас ставленныхполукругомколоннуходилаподпираемаягуртамисводакключуповторяяуловкустрельчатойаркиум еющейоперетьсянапустотувысшаястепеньлицемериявстатикеиуговоритьколоннычтоониобязаныпихатьввер хребрасводааребрамраспираемымдавлениемзамкавнушитьчтобониприжималикземлеколонныносводещехит реонявляетсяивсеминичемипричинойиследствиемвединомлицеоднакоямоментальнопонялчтоотворачивать сяотмаятникасвисающегососводаиразмышлятьвместоэтогоосводетожесамоечтозарекатьсяотродниканопить изисточникахорсоборасенмартендешансуществоваллишьблагодарятомучтоимелсуществованиевпрославлен иезаконамаятникамаятниксуществовалтолькопотомучтосуществовалсоборнесбежишьотбесконечностиподу маляудираякдругойбесконечностинеубережешьсяотвстречистождественнымпытаясьотыскатьиноепопрежне мунеотводяглазоткючасоборногосводаясталпятитьсяотступаяшагзашагомзавремяпрошедшеесмоментапри ходаядетальнозаучилрасположениезаладаимощныеметаллическиечерепахипатрулировавшиестеныпостоянн омаячиливуглуполязренияпропятившисьчерезвесьнефдовходнойдверияснованоказалсяподсеньюгрозныхпте родактилейизпроволокиитряпокзловещихстрекозневедомочьейоккультнойволейзасланныхподпотолокнефа онивыступалиметафорамизнаниязначительноболееглубокимичемвероятнозамышлялдидактразместившийи хвназидательнойпоследовательноститрепетаниенасекомыхирептилиймезозояаллегориябессчетныхмиграци ймаятниканадповерхностьюземлиархонтыизвращенныеэманациионипикировалинаменяцелясьархеоптерикс овымиклювамиаэропланыбрегеблериоэсногеликоптердюфопосетительконсерваторияанукиитехникивпариж епройдячерездворвосемнадцатоговекаипослеэтогонесколькокоридороввступаетвдревнююаббатскуюцерков ьврезаннуювболееновыйкомплексзданийподобнотомукакпреждеонабылаоблепленасовсехсторонстроениям иприоратапривходесразуперехватываетдухотстранногосоюзагорнейзапредельнойстрельчатостисхтоническ иммиромпожирателейсоляркиимазутапонизутянетсяпроцессиясамоходовсамокатовипаровыхэкипажейсвер хувисятвоздухоплавательныемашиныпионероводнипредметыцелыдругиеободраныистрепанывременемивсе онивместепредстаютподсмешанныместественнымиэлектрическимсветомкакбудтовпатиневлакеколлекцион нойвиолончелииногдасохраняетсятолькоскелетшассинаворотприводовирукоятейисулитнеописуемыепытки такивидишьсебяприкрученнымцепямикэтомуложуоткровенностивотвотоношевельнетсяпойдеткопатьтвоем ясоирытьсявжилахдополногоичистосердечногопризнания

Висновки: Під час виконання цього лабораторного практикуму отримано навички роботи з потоковими шифрами на прикладі шифру Віженера, шифрування ключами різних довжин. Шукати ключ за шифрованим текстом, розраховувати індекси відповідності.